MODELLING SEMANTICS OF SECURITY RISK ASSESSMENT FOR BRING YOUR OWN DEVICE USING METAMODELLING TECHNIQUE

ZAMHARIAH BINTI MD ZAIN

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

JULY 2018

ACKNOWLEDGEMENT

First of all, I am blessed and thankful to the Great Almighty, Allah for giving me the strength and the courage to complete this research. Here, I would also like to express my gratitude to everyone who supported, gave me the motivation and assisted me in completing this work. I would like to express my deep appreciation and indebtedness to my supervisor, Dr. Siti Hajar binti Othman and my co-supervisor, Puan Rashidah binti Kadir for their great collaboration, guidance, help, and endless support for this project. Without their help, I probably could not finish this thesis.

To my family, I am truly thankful and want to express my gratefulness especially for my lovely mother, father, brothers and sisters who always support me and being there for me despite the distance. They always gave me advices, and straightened my focus on study because at times, I felt depressed and lost. Their endless support, compassion and love has brought me the toughness, and conviction in facing allegations and challenges in doing my master.

I also want to express my appreciation and thanks to all my friends for their great companionships during my ups and down. With all truthfulness, they have encouraged, supported and helped me a lot in completing this Master Project. The completion of this research would not be possible without their participation and assistance.

ABSTRACT

Rapid changes in mobile computing devices or modern devices such as smartphones, tablets and iPads have encouraged employees to use their personal devices at workplace. Bring Your Own Devices (BYOD) phenomenon in an enterprise has become pervasive in demand for business purposes. Most organizations practice BYOD as it offers a wide variety of advantages such as increasing work productivity, reducing cost and giving employee's satisfaction. Despite that, BYOD practices trigger opportunities and challenges for the enterprise if there have no security policies, regulations and management on personal devices. Common BYOD security threats includes data leakage, exposure to malicious malware and sensitive corporates information. In this study, the Security-based BYOD Risk Assessment Metamodel (Security-based BYODRAM), a high-level knowledge structure was proposed for describing Security-based BYOD Risk Assessment domain. Review on thirty-five existing models which comprises of Risk Assessment and BYOD security models was done to identify the important concepts and semantic. Meta Object Facility (MOF) was the metamodeling language used in developing the metamodel. This study contributes a platform of incorporating and sharing of the Security-based BYOD Risk Assessment knowledge and giving solutions in managing BYOD security breaches. Real BYOD scenarios such as the Ottawa Hospital, privacy risks in enterprise and independent schools in Western Australian were used in demonstrating the semantics of proposed metamodel.

ABSTRAK

erubahan pesat dalam peranti pengkomputeran mudah alih atau peranti moden seperti telefon pintar, tablet dan iPad telah menggalakkan pekerja menggunakan peranti peribadi mereka di tempat kerja. Fenomena Bawa Peranti Anda Sendiri (BYOD) di perusahaan semakin meluas digunakan untuk tujuan perniagaan. Kebanyakan organisasi mengamalkan BYOD kerana terdapat pelbagai kelebihan seperti peningkatan produktiviti kerja, pengurangan kos dan kepuasan kepada pekerja. Namun begitu, BYOD boleh mencetuskan peluang dan cabaran bagi perusahaan jika tidak ada polisi keselamatan, peraturan dan pengurusan peranti peribadi yang digunakan dalam sesebuah organisasi. Amaran keselamatan dengan pelaksanaan BYOD umumnya termasuk kebocoran data, terdedah kepada ancaman perisian bahaya dan data korporat yang sensitif. Dalam kajian ini, Metamodel Keselamatan Berasaskan Penilaian Risiko BYOD (Keselamatan Berasaskan BYODRAM), iaitu struktur pengetahuan peringkat tinggi dicadangkan untuk menggambarkan domain Penilaian Risiko BYOD yang berasaskan Keselamatan. Kajian pada tiga puluh lima model sedia ada yang terdiri daripada model Penilaian Risiko dan model Keselamatan BYOD telah dijalankan untuk mengenal pasti konsep-konsep penting dan semantiknya. Meta Objek Fasiliti (MOF) adalah bahasa metamodel yang digunakan dalam pembangunan metamodel. Kajian ini menyumbang kepada platform menggabungkan dan berkongsi pengetahuan Penilaian Risiko BYOD yang berasaskan Keselamatan dan memberi penyelesaian dalam menguruskan pelanggaran keselamatan dalam BYOD. Senario-senario BYOD yang sebenar seperti Hospital Ottawa, risiko privasi dalam perusahaan dan sekolah swasta di Australia Barat telah digunakan untuk menunjukkan semantik metamodel yang dicadangkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATION

ASF	Android Security Framework
BYOD	Bring Your Own Devices
BYOD SF	BYOD Security Framework
BYODRA	BYOD Risk Assessment
BYODRAM	BYOD Risk Assessment Metamodel
BYOP	Bring Your Own Phone
BYOPC	Bring Your Own PC
BYOT	Bring Your Own Technology
CBA	Cost-Benefit Analysis
CCs	Cloud Clients
CSP	Cloud Service Provider
EMDSLC	Enterprise Mobile Device Solution Life Cycle
IRAM	Information Risk Assessment Methodology
IRM	Information Risk Management
ISA & ISS RA	Information Security Awareness and Information System Security Risk Assessment
IT SRM	Information Technology Security Risk Management
MAM	Mobile Application Management

MCM	Mobile Content Management
MDM	Mobile Device Management
MIF	Model Important Facility
MOF	Meta Object Facility
NAC	Network Access Control
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OiRA	Online Interactive Risk Assessment
OMG	Object Management Group
OSSF	Online Services Security Framework
PRA	Privacy Risk Assessment
RA	Risk Assessment
RAP	Risk Assessment Process
RMF	Risk Management Framework
RMP	Risk Management Process
SMM	Secure meta-market
SPM	Security Policy Model
SRA	Security Risk Assessment
SRAF	Security Risk Assessment Framework
SSEP	Security Systems Engineering Process
UML	Unified Modeling Language
VPN	Virtual Private Network
WLSA	White-List Security Architecture

LIST OF SYMBOLS

$\vec{w}$	-	Weighted average
w	-	Weight of the item
x	-	Values of the items
N	-	Sum of weight of the item
$\sum$	-	Sum

CHAPTER 1

INTRODUCTION

1.1 Overview

Bring Your Own Devices (BYOD) refers to a concept of allowing employees to use their own mobile devices such as smartphones, tablets, laptops and iPads for work purposes. Since 2012, the use of personal devices at workplace has become pervasive (Jamaluddin *et al.*, 2015). Many organizations implemented BYOD in their information technology management and it is increasing from time to time. BYOD allows employees to bring and use their own devices at work. In addition, BYOD usage is a good practice in many enterprises nowadays, since it can increase the quality of work, comfort and reduce cost for IT infrastructure management. However, even though BYOD brings many advantages in organization, there are also BYOD security issues faced by the employees. This caused challenges and difficulties to the security experts to manage the information of BYOD security (Fiorenza, 2014). Therefore, metamodelling technique has been chosen as the solution to structure and manage the knowledge of BYOD security risk. Security-based BYOD Risk Assessment Metamodel (BYODRAM) has been proposed to minimize the BYOD security problems in enterprises.

1.2 Problem Background

BYOD phenomenon is currently becoming more prevalent in the business industry and certain organizations. Based on the survey in Asia Pacific, there are more than 85% Malaysians who used their own devices at workplace and only 26% of them were provided with sufficient facilities by their IT department. Employees can also create, store, and manage the corporate data using the devices. Various types of personal devices used by employees at workplace such as smartphones, tablets, IPad, and laptops caused lots of security problems and until now there are no comprehensive guideline that could handle security risk in BYOD devices. Guidelines are general statements that are used in making achievement in the policy objectives (Souppaya and Scarfone, 2013). This is done by providing a framework to implement procedures.

Based on the research made, it is found that there is also faults with the existing models in assessing the BYOD risks. The existing models are developed to manage the risks but there are no exact Security-based BYODRAM that is developed to manage the BYOD security issues. There is a question on how to manage BYOD issues and challenges in enterprises (Shumate and Ketel, 2014). Based on this, the operational risk management should be implemented to avoid the operational risks since the operational risk may impact the implementation of strategic decisions. This includes the identifying, measuring, monitoring, reporting, controlling and mitigating the process. The analysis is also needed to determine the cost to fix operational risk problems and the loss due to the operational risk event (Basel Committee on Banking Supervision, 2001). Hence, it is a necessity to create generic representation of the knowledge in managing BYOD security risks. Therefore, metamodelling technique is found suitable in managing the knowledge of BYOD Risk Assessment (Othman, 2012).

One of the biggest problems related to BYOD adoption is data leakage. This is caused by corporate data that can be accessed through Wi-Fi connection and the transmission of data which is also not encrypted. The loss of mobile devices due to theft is the biggest risk by adopting BYOD that could be faced by enterprises

(AlHarty and Shawkat, 2013). If the employee lose their personal devices that stored corporate data, it can cause untrusted parties to retrieve all the private data inside the device (Wiech, 2013). All the sensitive information inside the devices might be accessed by the intruders and taken for specific purpose. Other than that, factor that contributes to data leakage is when the employee quit job from the company and it has high possibilities that the corporate data still remain inside their own devices (Wiech, 2013). It also been stated by Forrester (2012), that mobile devices security concerns with 65% is the biggest security challenge by deploying BYOD program. Angwin *et al*. (2011) mentioned that when employees access the network resource using mobile devices, outsiders can easily trace the personal information and corporate data.

According to the existing models of Security-based BYOD Risk Assessment, there is lacking of unified approach in security risk assessment. For example, one of the existing models which is Risk Assessment Process model which is developed to assess the information security risk (Ross, 2012). This model lacks of the BYOD security main components such as the Mobile Device Management (MDM), policy, access control, remote wiping, antivirus and anti-malware (Downer and Bhattacharya, 2016). So, the Security-based BYODRAM will be developed by integrating the BYOD security and assessment main components within the metamodel. So, this is the reason why an investigation of the existing models of risk assessments and BYOD security is required in order to extract all the main components of risk assessment and BYOD security concepts.

It is important to develop a comprehensive information system that stores and manages the BYOD security related issues. The BYOD domain users will have a knowledge of hazards and the risk level of specific BYOD risks. Besides, this knowledge-based system recommend security controls in handling specific BYOD issues. The organization must have a standard guideline on managing BYOD risk related problems because it requires variety of business process in solving the risks. The complexity of the user to access the knowledge of BYOD security risk will be ease with the metamodel. This proposed metamodel support the user of BYOD domain such as expert, security manager, and officer in making decisions of the related security issues.

BYOD policy is becoming a serious phenomenon when it affects the information security risks of the employer's information such as report, preserve data and data leakage. BYOD implementation causes greatest challenge in organizations when the confidential data is not managed strategically by the organization itself (Olalere *et al.*, 2015). Referring to this, BYOD policy should complement other information security and governance policies. Personal mobile devices usage among workers causes security issues problem as workers commonly will carry their own devices which contain private and confidential data everywhere (Broomfield, 2006). The security requirement should be provided for mobile devices such as authentication, transmission encryption requirements, wipe devices system, right to manage, monitor and wipe devices, support model, company liability, restrict the usage of devices, acceptable use and practices for mobile data usage on international travel (EY, 2013).

The existing models of Security-based BYOD risks assessment also lacks the BYOD security components in its implementation. Based on the existing models, the protection of internal network resources should be enhanced; for example the Virtual Private Network (VPN), access control, and firewalls. For example, BYOD Security model lacking of security protection within the company network services. It only provides limited security protection in the channel of communication through VPN (Ali *et al.*, 2016). So, this revealed the needs and importance of managing BYOD security knowledge. Due to this, the enhancement of the Security-based BYOD Risk Assessment will be done to ensure the improvement of BYOD security and risk assessment components in assessing risks.

The metamodel technique is chosen in managing the BYOD security risks problems. Based on this, metamodelling is needed in minimizing the BYOD risks. The metamodel plays its role in supporting the engineering design optimization. Intensive research has also been done in deploying metamodelling techniques in design and optimization. Metamodelling can be used in problem formulation. According to this, the metamodel is used to solve the complex domain. Any domain which has shared key-points need metamodelling to integrate it into one platform. Next is metamodelling can play a role in model approximation, which is used in approximation of computation-intensive process across the whole design space

aimed to reduce the computational cost. Besides, metamodelling has the ability to allow modellers to structure, organize, and manage any domain knowledge to solve the interoperability's issues. (Wang and Shan, 2007).

In addition, malicious malware is also one of the most challenging security risks engaged to BYOD. Adopting BYOD may bring malware and viruses to the company network. Malware is the attack that is based on the malicious applications that are able to affect both the devices and the applications inside devices (Olalere *et al.*, 2015). Mobile malware consists of the applications that is embedded with code inside and compromised with the security of devices (Morrow, 2012). In 2012, there is Shamoon malware that inactivate more than 30,000 computers and also stole data of the national oil company, Saudi Aramco in Saudi Arabia (Armando *et al.*, 2014). In March 2013, at the top three South Korean banks and the country's two largest broadcaster computer networks were down caused by malicious malware (Fielder, 2013).

Enterprise needs a standard guideline in handling the security risks issues. Based on the review made on the existing models, there are lacking of risk assessment components such as risk specification, risk analysis, and risk evaluation. Risk specification is used to determine the risk factors of BYOD and they are extracted from a comprehensive viewpoint by using the Risk Breakdown Structure (RBS) method. For risk analysis, risk matrix method is used and it consists of four countermeasures in accordance with their probability and risk impact such as risk transferences, risk mitigation, risk acceptance and risk avoidance. For the risk evaluation, it determines the countermeasures based on the risk factors that are investigated (Tanimoto *et al.*, 2016). By using a metamodel form, an integrated view of all important phases involving Security-based BYOD Risk Assessment will be analysed and determined. The security risks which is engaged to the BYOD adoption can be minimized by considering all the important phases in Security-based BYOD Risk Assessment. This is one factor why metamodel is chosen to manage the BYOD risks problems (Othman, 2012).

1.3 Problem Statement

Although BYOD brings advantages, there also security risks impact faced by companies when implementing BYOD. Besides, there are no existing Security-based BYODRAM that can be used as references. So, the appropriate guideline must be strategically developed and implemented to minimize the BYOD risks. The guideline is important for managing the security of BYOD risks. All the important concepts needed in assessing the BYOD risks which is security risk assessment concepts should be considered. This study plans to enhance the security in the risk assessment approach of BYOD risks. Therefore, the questions are how to assess the BYOD risks and what is the appropriate procedure?

The following are research questions of this research:

i) What is the important elements in the Security-based BYOD risk assessment domain?
ii) How to assess BYOD risk with Security-based BYODRAM?
iii) What technique will be used to validate the developed Security-based BYODRAM for assessing BYOD risks?

1.4 Research Aim

This research aims to manage knowledge of how security risk assessment in BYOD domain should be conducted through a high level knowledge structure, a metamodel. This approach is important as it could allow domain users in making decisions when they face various types of BYOD risks.

1.5 Research Objectives

The objectives are stated as follows:

i) To identify the security risk assessment important concepts for BYOD domain from existing sources.

ii) To use the metamodelling approach in developing the Security-based BYODRAM in assessing BYOD risks.

iii) To validate the Security-based BYODRAM by using metamodel validation techniques.

1.6 Research Questions, Objectives and Deliverables of this Research

Table 1.1 represents the research questions, objectives and deliverables of this research.

Table 1.1: Research questions, objectives and deliverables

Research Question	Objective	Deliverable
i) What is the important elements in the Security-based BYOD risk assessment domain?	i) To identify the security risk assessment important concepts for BYOD domain from existing sources.	i) BYOD concepts
ii) How to assess BYOD risk with Security-based BYODRAM?	ii) To use the metamodelling approach in developing the Security-based BYODRAM in assessing BYOD risks.	ii) BYOD metamodel
iii) What technique will be used to validate the developed Security-based BYODRAM for assessing BYOD risks?	iii) To validate the BYODRAM by using metamodel validation techniques.	iii) A validated BYODRAM

1.7 Research Scope

The scope of the research is limited to the following, namely:

i) This study focuses on the development of the Security-based BYODRAM with the important elements needed in assessing BYOD risks based on the existing security risk assessment models.

ii) This study focus on the enhancement of the lackings in the existing models in the BYOD security risks context.

iii) This research used two techniques in validating the metamodel to manage the knowledge of BYOD security risks, but in this research, we used the metamodel technique. Two validation techniques are used in validating the proposed Security-based BYODRAM. The first one is Expert Review *(Face Validity)* and another one is Case Study *(Tracing)* techniques.

1.8 Summary

In this chapter, the preliminary study for the research has been discussed. The introduction, background and problem of the study was described to give more information and understanding about the research that was conducted. Besides, there was a discussion on project aims and objectives that provided clear information on things that were focused in this research. Next, the project scopes also gave information about the limitations of the research. In the next chapter, discussion is about the literature review which includes the analysis of the existing model collection.

REFERENCES

2011. Internet Security Threat Report. Symantec, April 2012. [Online]. Available: www.symantec. com/threatreport. [Accessed 2 February 2016].

Ab Rahman, N.H. and Choo, K.K.R., 2015. A survey of information security incident handling in the cloud. *Computers and Security*, 49, pp.45–69.

Alberts, C.J. and Dorofee, A.J., 2010. Risk Management Framework: DTIC Document.

Ali, S., Qureshi, M.N. and Abbasi, A.G., 2016. Analysis of BYOD security frameworks. *Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015*, pp.56–61.

Almorsy, M., Grundy, J. and Ibrahim, A.S., 2011, July. Collaboration-based cloud computing security management framework. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on* (pp. 364-371). IEEE.

Angwin, J. and Valentino-Devries, J., 2011. Apple, Google collect user data. *The Wall Street Journal*.

Arcaini, P., Gargantini, A., Riccobene, E. and Scandurra, P., 2012. Formal semantics for metamodel-based domain specific languages. *Formal and Practical Aspects of Domain-Specific Languages: Recent Developments*, pp.216–241.

Armando, A., Costa, G. and Merlo, A., 2013. Bring your own device, securely. *Proceedings of the 28th Annual ACM Symposium on Applied Computing - SAC '13*, p.1852.

Armando, A., Costa, G., Verderame, L. and Merlo, A., 2014. Securing the "Bring your own device" paradigm. *Computer*, 47(6), pp.48–56.

Armando, A., Merlo, A. and Verderame, L., 2014. Security considerations related to the use of mobile devices in the operation of critical infrastructures. *International Journal of Critical Infrastructure Protection*, 7(4), pp.247–256.

At, F.U.S., 2016. Enterprise Mobile Threat Report Table of Contents. , pp.1–34.

Bakhtiyari Shahri, A., 2012. A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. *Journal of Information Security*, 03(02), pp.169–176.

Bann, L.L., Singh, M.M. and Samsudin, A., 2015. Trusted Security Policies for Tackling Advanced Persistent Threat via Spear Phishing in BYOD Environment. *Procedia Computer Science*, 72, pp.129–136.

Baras, D.S.A., Othman, S.H., Ahmad, M.N. and Ithnin, N., 2015. Towards managing information security knowledge through metamodelling approach. *Proceedings - 2014 International Symposium on Biometrics and Security Technologies, ISBAST 2014*, pp.310–315.

Barua, A., 2013. Methods for Decision-Making in Survey Questionnaires Based on Likert Scale. *Journal of Asian Scientific Research*, 3(1), pp.35–38.

BEERS, W. C. M. V. 2005. Kriging Metamodelling For Simulation. PhD, Tilburg University.

Bermell-Garcia, P., 2007. A metamodel to annotate knowledge based engineering codes as enterprise knowledge resources.

Bernstein. 1999. Using Meta-Data to Conquer Database Complexity Colloquium Presentation.

Beydoun, G., Low, G., Mouratidis, H. and Henderson-Sellers, B., 2009. A security-aware metamodel for multi-agent systems (MAS). *Information and Software Technology*, 51(5), pp.832–845.

Börger, E., 2002. The origins and the development of the ASM method for high level system design and analysis. *Journal of Universal Computer Science*, 8(1), pp.2–74.

Boyens, J., Paulsen, C., Moorthy, R. and Bartol, N., 2015. Supply Chain Risk Management Practices for Federal Information Systems and Organizations. *NIST Special publication*, p.282.

Bryant, B.R. et al., 2011. Challenges and directions in formalizing the semantics of modeling languages. *Computer Science and Information Systems*, 8(2), pp.225–253.

Burt J. BYOD trend pressures corporate networks. eweek 2011;28(14):30–1.

[Online]. Available: http://www.zdnet.com/byod-on-rise-in-asia-but-challenges-remain-7000010660/ [Accessed 2 February 2016].

C. Tzoumas, “The BYOD World.” in BusinessWest, 2013, vol. 30, no. 2, p. 45.

Calder, A. and Watkins, S.G. 2010. Information Security Risk Management for ISO27001/ISO27002. Cambridgeshire: IT Governance Ltd.

Caralli, R.a. C.R., Stevens, J.J.F., Young, L.L.R. and Wilson, W.W.R., 2007. Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. *Young*, (May), pp.1–113.

Carlson, C., Hutton, A. and Gilliam, A., 2010. *Technical Guide FAIR – ISO / IEC 27005 Cookbook*

Cho, M.G., 2015. Air force institute of technology. *Transformation*, (June).

Cicchetti, A., Ruscio, D.D., Kolovos, D.S. and Pierantonio, A., 2011. A test-driven approach for metamodel development. *Emerging Technologies for the Evolution and Maintenance of Software Models*, pp.319-342.

CISCO. 2012. *CISCO BYOD Smart Solution.*

Cisco Systems Inc., 2014. Cisco Enterprise Mobility Solution: Device Freedom Without Compromising the IT Network. , p.23.

Clark, T., Evans, A. and Kent, S., 2002. Engineering modelling languages: A precise meta-modelling approach. *Fundamental Approaches to Software Engineering*, p.159.

Colomb, R., Raymond, K., Hart, L., Emery, P., Welty, C., Xie, G. T., & Kendall, E. 2006. The object management group ontology definition metamodel. In *Ontologies for software engineering and software technology*(pp. 217-247). Springer Berlin Heidelberg.

Damenu, T.K. and Balakrishna, C., 2015. Cloud Security Risk Management: A Critical Review. *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*, pp.370–375.

de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., García-Sánchez, P., & Fernández-Ares, A. 2015. Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications*, *68*, 83-95.

Downer, K. and Bhattacharya, M., 2016. BYOD security: A new business challenge. *Proceedings - 2015 IEEE International Conference on Smart City, SmartCity 2015, Held Jointly with 8th IEEE International Conference on Social*

Computing and Networking, SocialCom 2015, 5th IEEE International Conference on Sustainable Computing and Communic, pp.1128–1133.

Emerson, M. and Sztipanovits, J., 2006. Techniques for Metamodel Composition. *OOPSLA–6th Workshop on Domain Specific Modeling*, (November), pp.123–139.

EY, 2013. Security and risk considerations for your mobile device program. *Insights on governance, risk and compliance*, (September), p.12.

Favre, L. ed., 2010. *Model Driven Architecture for Reverse Engineering Technologies: Strategic Directions and System Evolution: Strategic Directions and System Evolution*. IGI Global.

Fielder, Tales from the darkside: Mobile malware brings down Korean banks, RSA Security Analytics, March 21, 2013

Flores, D.A., Bring Your Own Disclosure : An Analysis of BYOD Threats to Corporate Information.

French, A., Guo, C. and Shim, J.P., 2014. Current Status, Issues and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, 35(11), p.10.

French, A. M., Guo, C., & Shim, J. P. 2014. Current status, issues, and future of bring your own device (BYOD). *Communications of the Association for Information Systems*, *35*(10), 191-197.

Friginal, J., Guiochet, J. and Killijian, M.O., 2014. Towards a privacy risk assessment methodology for location-based systems. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 131, pp.748–753.

Fujitsu. 2013. Bring & Your & Own & Device : Bring & Your & Own & Device : , (November), pp.1–8.

Gaines, J. and Martin, E., 2014. Bring & Your & Own & Device : Bring & Your & Own & Device : , (November), pp.1–8.

Gallotto, S. and Chen, W., Security Management of Bring-Your-Own-Devices.

Garba, A.B., Armarego, J. and Murray, D., 2015. A Policy-Based Framework for Managing BYOD Environments. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 4(2), pp.189–198.

Gargantini, A., Riccobene, E. and Scandurra, P., 2009. A semantic framework for

metamodel-based languages. *Automated Software Engineering*, 16(3–4), pp.415–454.

Gens, F., Levitas, D. and Sega, R., 2011. 2011 Consumerization of IT Study : Closing the " Consumerization Gap ." *Idc*, 1156, pp.1–21.

Ghosh, A., Gajar, P.K. and Rai, S., 2013. Bring Your Own Device (Byod): Security Risks and Mitigating Strategies. *Journal of Global Research in Computer Science*, 4(4), pp.62–70.

GNU Team, 2008. GNU Scientific Library. *International Urology and Nephrology*, 40(1), pp.249–253.

Goldstein, A. and Frank, U., 2016. Components of a multi-perspective modeling method for designing and managing IT security systems. *Information Systems and e-Business Management*, 14(1), pp.101–140.

Google. Good to know e a guide to staying safe and secure online [WWW Document]. [Online]. Available: http://www.google.com/ goodtoknow/online-safety/locking/. [Accessed 12 March 2017].

Hasan Albakri, S. et al., 2014. Traditional Security Risk Assessment Methods in Cloud Computing Environment: Usability Analysis. *1st International Conference of Recent Trends in Information and Communication Technologies Traditional*, (November 2015), pp.483–495.

Henderson-Sellers, B., 2011. Bridging metamodels and ontologies in software engineering. *Journal of Systems and Software*, *84*(2), pp.301-313.

Hevner, A. and Chatterjee, S., 2010. *Design Science Research in Information Systems*.

Hjalmarsson, A. and Rudmark, D., 2012. Designing digital innovation contests. *Conference on Design Science Research in …*, pp.9–27.

Hnetynka, P., and Plasil, F. 2004. "Distributed Versioning Model for MOF". In *Proceedings of the winter international synposium on Information and communication technologies* (pp. 1-6). Trinity College Dublin.

Hutchison, D. and Mitchell, J.C., 2011. *Lecture Notes in Computer Science*.

ISACA, Advanced Persistent Threat Awareness Study Results, [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/wp_apt-survey-report.pdf [Accessed 26 September 2016].

Jakobsson, U., 2004. Statistical presentation and analysis of ordinal data in nursing research. *Scandinavian Journal of Caring Sciences*, 18(4), pp.437–440.

Jamaluddin, H., Ahmad, Z., Alias, M. and Simun, M., 2015. Personal Internet Use: The Use of Personal Mobile Devices at the Workplace. *Procedia - Social and Behavioral Sciences*, 172, pp.495–502.

Jiang, X. 2011. Security alert: New sophisticated android malware droidkungfu found in alternative chinese app markets.

Johns, R., 2010. SQB Methods Fact Sheet 1: Likert Items and Scales. , 1(March), pp.1–11.

Karagiannis, D.; Kühn, H., 2002. Metamodelling Platforms. *Proceedings of the Third International Conference EC-Web 2002 –*, p.182.

Kassab, M., Ormandjieva, O. and Daneva, M., 2009, March. A metamodel for tracing non-functional requirements. In *Computer Science and Information Engineering, 2009 WRI World Congress on* (Vol. 7, pp. 687-694). IEEE.

Kent, K. and Souppaya, M., 2006. Guide to Computer Security Log Management. *National Institute of Standards and Technology*, pp.1–72.

Kim, K. J., & Hong, S. P. 2013. Study on Enhancing Vulnerability Evaluations for BYOD Security. *International Journal of Security and Its Applications*, *8*(4), 229-238.

Kissel, R., Scholl, M., Skolochenko, S. and Li, X., 2006. Guidelines for Media Sanitization. *NIST Special Publication 800-88*, 800, pp.16–27.

Kitson, A.L. et al., 2008. Evaluating the successful implementation of evidence into practice using the PARiHS framework: Theoretical and practical challenges. *Implementation Science*, 3(1), pp.1–12.

Krehel, O. 2011. Worse than zombies: the mobile botnets are coming.

Landoll, D.J., 2006. *The Security Risk Assessment Handbook:A Complete Guide for Performing Security Risk Assessments*,

Lee, J., Lee, Y. and Kim, S.C., 2013. A White-List based Security Architecture (WLSA) for the safe mobile office in the BYOD era. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7861 LNCS, pp.860–865.

Lee, K., Tolentino, R. S., Park, G. C., & Kim, Y. T. 2010. A study on architecture of

malicious code blocking scheme with white list in smartphone environment. In *Communication and Networking* (pp. 155-163). Springer Berlin Heidelberg.

Liu, Y., Höglund, S., Khan, A. H., & Porres, I. 2010. A feasibility study on the validation of domain specific languages using owl 2 reasoners. In*Proceedings of the 3rd Workshop on Transforming and Weaving Ontologies in Model Driven Engineering Malaga, Spain. CEUR Workshop Preceedings, CEUR*.

Lund, M. S., Solhaug, B., & Stølen, K. 2010. *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media.

Macedo, F., & da Silva, M. M. Comparative Study of Information Security Risk Assessment Models.

Mahesh, S., & Hooter, A. 2013. *Managing and securing business networks in the smartphone era* (Management Faculty Publications, Paper 5).

Mansfield-Devine, S. 2012. Interview: BYOD and the enterprise network. *Computer fraud & security*, *2012*(4), 14-17.

Marjanovic, Z., 2013. Effectiveness of security controls in BYOD environments. *The University of Melbourne.* [Online]. Available: *http://hdl. handle. net/11343/33346*. [Accessed 11 May 2017].

Marshall, S., 2014. IT Consumerization: A Case Study of BYOD in a Healthcare Setting. *Technology Innovation Management Review*, 4(3), pp.14–18.

Meckesheimer, M. and Booker, A. J. 2002. Computationally Inexpensive Metamodel Assessment Strategies. AIAA JOURNAL. 40(10): 2053-2060.

Mejias, R.J., 2012. An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. *2012 45th Hawaii International Conference on System Sciences*, (January 2012), pp.3258–3267.

Meszaros, J. and Buchalcevova, A., 2017. Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security*, 65, pp.300–313.

Miller, K.W., Voas, J. and Hurlburt, G.F., 2012. BYOD: Security and privacy considerations. *IT Professional*, 14(5), pp.53–55.

MOF, O., 2002. OMG Meta Object Facility (MOF) Specification v1. 4.

Mr. Vishal Gupta Deepak Sangroha, L.D., 2013. An Approch to Implement Bring Your Own Device(BYOD) Securely. *Ijecce*, 4(2), pp.154–156.

Nadkarni, P.M., 2011. *Metadata-driven Software Systems in Biomedicine*.

Neff, T., 2013. A winning BYOD policy balances usability & control. *Compliance Week*, *10*(109), p.42.

Neto, F., Manuel, J., da Silva, M.M. and Delgado, J., 2009. Models for Assessing Information Security Risk Engenharia Informática e de Computadores. , pp.1–64.

Networks, M., BYOD Best Practices.

Nicholas, J.P., Response of Microsoft Corporation to Request for Information. , 98052(425).

Olalere, M., Abdullah, M.T., Mahmod, R. and Abdullah, A., 2015. A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 5(2), p.2158244015580372-.

Othman, S.H. and Beydoun, G., 2010. Metamodelling Approach To Support Disaster Management Knowledge Sharing. *ACIS 2010 Proceedings*, 2010, pp.1–10.

Othman, S.H., 2012. Metamodelling Approach for Managing Disaster Management Knowledge.

Othman, S.H., Beydoun, G. and Sugumaran, V., 2014. Development and validation of a Disaster Management Metamodel (DMM). *Information Processing and Management*, 50(2), pp.235–271.

Ovum. (2012, 5 17). *International Data Privacy Legislation Review: A Guide for BYOD Policies.*

Pegrum, M., Oakley, G. and Faulkner, R., 2013. Schools going mobile: A study of the adoption of mobile handheld technologies in western australian independent schools. *Australasian Journal of Educational Technology*, 29(1), pp.66–81.

Purdy, G., 2010. ISO 31000:2009 - Setting a new standard for risk management: Perspective. *Risk Analysis*, 30(6), pp.881–886.

Qing, L. Y. (2013). BYOD on rise in Asia, but challenges remain. *ZDNet*.

Rivera, D., George, G., Peter, P., Muralidharan, S. and Khanum, S., 2013. Analysis of security controls for BYOD (bring your own device). *Melbourne: The University of Melbourne*.

Romer, H., 2014. Best practices for BYOD security. *Computer Fraud and Security*, 2014(1), pp.13–15.

Ross, R.S., 2012. Guide for Conducting Risk Assessments. *Special Publication (NIST SP) - 800-30 Rev 1*, (September), p.95.

Sabatier, P.A. et al., 1999. *Theories of the Policy Process*,

Sans, 2013. " Your Pad or Mine ?"

Sargent, R.G., 2005. Verification and Validation of Simulation Models. *Proceedings of the 37th Winter Simulation Conference (WSC'05)*, pp.130–143.

Saripalli, P. and Walters, B., 2010. QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. *2010 IEEE 3rd International Conference on Cloud Computing*, pp.280–288.

Schmidt, D.C., 2006. Model-Driven Engineering. *IEEE Computer*, 39(2), pp.25–31.

Science, N., 2013. An Expert System for Risk Assessment of Information System Security Based on ISO. , pp.56–61.

Shakhnov, V.A., Zinchenko, L.A., Rezchikova, E. V. and Glushko, A.A., 2015. An opportunity in engineering education: Russian BYOD tendencies: BMSTU case study. *Proceedings of 2015 International Conference on Interactive Collaborative Learning, ICL 2015*, (September), pp.299–304.

Sharples, M., Adams, A., Alozie, N., Ferguson, R., FitzGerald, E., Gaved, M., McAndrew, P., Means, B., Remold, J., Rienties, B. and Roschelle, J., 2015. Innovating pedagogy 2015: open university innovation report 4.

Shumate, T. and Ketel, M., 2014. Bring Your Own Device: Benefits, risks and control techniques. *Ieee Southeastcon 2014*, pp.1–6.

Singh, N. (2012). BYOD genie is out of the bottle–"Devil or angel". *Journal of Business Management & Social Sciences Research*, *1*(3), 1-12.

Souppaya, M. and Scarfone, K., 2013. Guidelines for Managing the Security of Mobile Devices in the Enterprise. *NIST Special Publication 800-124, Revision 1*, pp.1–30.

Sprinkle, J., Mernik, M., Tolvanen, J.P. and Spinellis, D., 2009. Guest editors' introduction: What kinds of nails need a domain-specific hammer? *IEEE Software*, 26(4), pp.15–18.

Sprinkle, J., Rumpe, B., Vangheluwe, H. and Karsai, G., H. (2010). Metamodelling State of the Art and Research Challenges 57–76.

Stueckle, J., 2011. *Android Protection Mechanism: A Signed Code Security Mechanism for Smartphone Applications* (No. Afit/Gce/Eng/11-06). Air

Force Inst Of Tech Wright-Patterson AFB Oh School Of Engineering And Management.

Tanimoto, S. et al., 2016. Risk assessment of BYOD: Bring your own device. *2016 IEEE 5th Global Conference on Consumer Electronics*, pp.1–4.

Thomson, G., 2012. BYOD: Enabling the chaos. *Network Security*, 2012(2), pp.5–8.

Tokuyoshi, B. 2013. The security implications of BYOD. *Network Security*, *2013*(4), 12–13.

Touche, D. 2011. Raising the bar, TMT Global Security Study-Key Findings.*Report published by Deloitte, 24p*.

Tu, Z., Yuan, Y. and Archer, N., 2014. Understanding user behaviour in coping with security threats of mobile device loss and theft. *International Journal of Mobile Communications*, *12*(6), pp.603-623.

Vahidov, R., 2006. Design Researcher's IS Artifact: a Representational Framework. *Proceedings of the 1st International Conference on Design Science Research in Information Systems and Technology*, pp.19–33.

Van Der Meulen, R. and Rivera J. 2013. 'Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes'. Gartner Inc. [Online]. Available: http://www.gartner.com/newsroom/id/2466615 [Accessed 2 February 2016].

Wang, G.G. and Shan, S., 2007. Review of Metamodeling Techniques in Support of Engineering Design Optimization. *Journal of Mechanical Design*, 129(4), p.370.

Xiang, C., Binxing, F., Lihua, Y., Xiaoyi, L., & Tianning, Z. 2011. Andbot: towards advanced mobile botnets. In *Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats* (pp. 11-11). USENIX Association.

Zahadat, N., Blessner, P., Blackburn, T. and Olson, B. a., 2015. BYOD security engineering: a framework & its analysis. *Computers & Security*, 55, pp.81–99.

Zhang, X., Wuwong, N., Li, H. and Zhang, X., 2010. Information Security Risk Management Framework for the Cloud Computing Environments. *2010 10th IEEE International Conference on Computer and Information Technology*, (2007), pp.1328–1334.